UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/889,524	02/28/2002	Dan Butnaru	09669/004001	5237

22511 7590 09/20/2005

OSHA LIANG L.L.P.
1221 MCKINNEY STREET
SUITE 2800
HOUSTON, TX 77010

EXAMINER
HENNING, MATTHEW T

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 09/20/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

TH

Office Action Summary	Application No.	Applicant(s)	
	09/889,524	BUTNARU ET AL.	
	Examiner	Art Unit	
	Matthew T. Henning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 July 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 February 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

This action is in response to the communication filed on 7/6/2005.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 7/6/2005 has been entered.

Response to Arguments

Applicant's arguments with respect to claims 2-23 have been considered but are moot in view of the new ground(s) of rejection.

Claims 2-23 have been examined.

All objections and rejections not set forth below have been withdrawn.

Specification

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

The abstract of the disclosure as amended is objected to because

Lines 4 and 8 contain legal phraseology ("said"), which must be removed.

Correction is required. See MPEP § 608.01(b).

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 9-10, and 16-17 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 9 recites the limitation "said key". The ordinary person skilled in the art would be unable to determine if this recitation was meant to refer to the "transport key", the "operation key" or the "application key". As such claim 9 and dependant claim 10 are rejected for failing to particularly point out and distinctly claim the subject matter which the applicant's regard as the invention.

Claim 16 recites the limitation "the operation key temporarily saved within a second volatile memory of the first unit" in lines 2-3. There is insufficient antecedent basis for this limitation in the claim.

Claim 17 recites the limitation "the operation key temporarily saved within a second volatile memory of the first unit" in lines 2-3. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 2, 4-6, 8-10, 13-17, 19-20, and 23 are rejected under 35 U.S.C. 102(b) as being anticipated by Bestock et al. (US Patent Number 4,933,971) hereinafter referred to as Bestock.

Regarding claim 20, Bestock disclosed a method for customizing a set of several second security units (See Bestock Fig. 2 and abstract), comprising:

secure downloading of an application key from a first security unit of a central processing unit to said set of second security units (See Bestock Fig. 2 and Abstract), said first unit and second units each comprising at least one memory (See Bestock Col. 7 Lines 48-53), wherein the method further comprises for each second unit in said set:

on each downloading, computing an operation key (KEK) in the first unit based on information specific to the second unit (KDT_0), a transport key (Transport Number), and a diversification algorithm (XOR) (See Bestock Col. 7 Paragraph 4, Col. 8 Paragraph 5, and Col. 11 Paragraph 2), said transport key residing within the memory of the first security unit, said memory being non volatile (See Bestock Col. 7 Lines 22-30);

encrypting the application key (KDT_1) in the first unit based on information comprising said operation key and an encryption algorithm (See Bestock Col. 8 Lines 55-62);

sending data comprising the encrypted application key to the second unit (See Bestock Col. 8 Lines 55-62);

on each downloading, computing an operation key (KEK_0) in the second unit based on information specific to the second unit (KDT_0), the transport key (Variant Number) and the diversification algorithm (XOR) (See Bestock Col. 7 Lines 6-22 and Col. 11 Paragraph 2), the same transport key residing in the non-volatile memory of each second security unit of said set (See Bestock Col. 7 Lines 17-30), said operation key not being stored within the memory of said second unit (See Col. 7 Lines 6-22); and

decrypting the encrypted application key in the second unit based on information comprising said operation key and a decryption algorithm which is the inverse of the encryption algorithm (See Bestock Col. 8 Line 63 – Col. 9 Line 8),

wherein said transport key residing within the memory of the first unit is present in the memory of the first unit prior to communicating with the second unit and the same transport key residing in the non-volatile memory of each second unit is present in the non-volatile memory of the second security unit prior to communicating with the first unit (See Bestock Col. 6 Lines 32-37 and Col. 7 Lines 17-30).

Regarding claim 2, Bestock disclosed sending information specific to the second unit to the first unit before computing the application key in the first unit (See Bestock Col. 7 Lines 31-41).

Regarding claim 4, Bestock disclosed sending information pertaining to an application key to the first unit, before encrypting the application key within said first unit (See Bestock Col. 7 Lines 31-41).

Regarding claim 5, Bestock disclosed choosing the application key to be encrypted based on said information pertaining to an application key (See Bestock Col. 8 Lines 45-49).

Regarding claim 6, Bestock disclosed that the encryption of an application key intended for a second unit is unique (See Bestock Col. 8 Lines 55-62).

Regarding claim 8, Bestock disclosed sending information pertaining to an application key to the second unit, before decrypting the encrypted application key within said second unit of said set (See Bestock Col. 8 Lines 55-62).

Regarding claim 9, Bestock disclosed storing within the second unit, after decrypting the encrypted application key, said key within said second unit (See Bestock Col. 8 Line 63 – Col. 9 Line 8).

Regarding claim 10, Bestock disclosed that storing of the application key within the second unit is done based on information pertaining to an application key (See Bestock Col. 8 Line 63 – Col. 9 Line 8).

Regarding claim 13, Bestock disclosed that the memory comprises a rewritable memory (See Bestock Col. 8 Line 63 – Col. 9 Line 8).

Regarding claim 14, Bestock disclosed that a second unit comprises several application keys (See Bestock Col. 8 Line 63 – Col. 9 Line 8).

Regarding claim 15, Bestock disclosed that the first unit comprises several application keys (See Bestock Col. 7 Lines 46-50).

Regarding claim 16, Bestock disclosed that after encrypting the application key, erasing the operation key temporarily saved within the second volatile memory of the first unit (See Bestock Col. 8 Lines 55-68).

Regarding claim 17, Bestock disclosed that after decrypting the application key, erasing the operation key temporarily saved within the second volatile memory of the first unit (See Bestock Col. 8 Lines 55-68).

Regarding claims 19 and 23, Bestock disclosed sending the encrypted application key and the information pertaining to an application key to the second unit by means of a single second command (See Bestock Col. 8 Lines 55-62).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> *A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.*

Claims 3, 18, and 21-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bestock as applied to claims 20, and 2-4 above respectively, and further in view of Menezes et al. ("Handbook of Applied Cryptography") hereinafter referred to as Menezes.

Bestock disclosed sending information pertaining to an application key (See Bestock Col. 7 Lines 58-61), and information specific to the second unit (See Bestock Col. 7 Lines 38-41) to

the first unit by means of a first single command (See Bestock Fig. 2 Step 36), but failed to disclose sending random information as well.

Menezes teaches a method for strong authentication in which a random number is sent from one entity to another along with a message, and the second entity sends the random number back to the first in the next communication (See Menezes Page 398 Section (i)).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Menezes in the keying system of Bestock by sending a random number with the message sent from the terminal to the host in order to authenticate the host. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect against replay and interleaving attacks against the system.

Claims 7 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bestock as applied to claim 20 above, and further in view of Sullivan et al. (US Patent Number 6,069,647) hereinafter referred to as Sullivan.

Bestock disclosed exchanging an application key (See Bestock Col. 8 Lines 55-62), but failed to disclose verifying the integrity of the key at receipt or the authenticity of the key at receipt.

Sullivan teaches that data should be digitally signed in order to verify the integrity and authenticity of the data (See Sullivan Col. 3 Paragraph 4).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Sullivan in the key exchange system of Bestock by digitally signing the key at the host prior to sending the key and then verifying the signature at the terminal upon receipt. This would have been obvious because the ordinary person skilled in the

art would have been motivated to protect against illicit modification of the key data prior to the terminal receiving the key.

Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bestock as applied to claim 20 above, and further in view of Blaze (US Patent Number 5,696,823).

Bestock disclosed storing keys at the host (See Bestock Col. 7 Lines 46-54) but failed to disclose the host comprising a smartcard.

Blaze teaches that smartcards can be used to store keys (See Blaze Col. 1 Lines 11-16).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Blaze in the key exchange system of Bestock by storing the keys in a smartcard. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect against illicit access to the keys by, for example, tampering.

Conclusion

Claims 2-23 have been rejected.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Matthew Henning
Assistant Examiner
Art Unit 2131
9/15/2005

AVAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100